

Autonomous Vehicle Cybersecurity Development Lifecycle (AVCDL) OASIS SARIF Presentation

Charles Wilson
Senior Principal Engineer, Cybersecurity Development Lifecycle Practice

version 1
2022-11-10

This work was created by **Motional** and is licensed under the **Creative Commons Attribution-Share Alike (CC BY-SA-4.0)** License.
<https://creativecommons.org/licenses/by/4.0/legalcode>

Reference Sources



NIST CYBERSECURITY WHITE PAPER (DRAFT) [CSCRS.NIST.GOV](https://www.nist.gov)

1 Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)

2
3
4

5 Donna Dodson
6 Applied Cybersecurity Division
7 Information Technology Laboratory
8
9 Murugiah Souppaya
10 Computer Security Division
11 Information Technology Laboratory
12
13 Karen Scarfone
14 Scarfone Cybersecurity
15 Clifton, VA
16

17
18 June 11, 2019
19
20
21
22

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-181

National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework

William Newhouse
Stephanie Keith
Benjamin Scribner
Greg Witte

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-181>

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Downloaded from SAE International by Charles Wilson, Friday, September 11, 2020

SAE INTERNATIONAL	SURFACE VEHICLE STANDARD	ISO/SAE 21434
	Road Vehicles - Cybersecurity Engineering	Issued 2021-09

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

SAE International is a global association of more than 128,000 engineers and related technical experts in the aerospace, automotive and commercial-vehicle industries. Standards from SAE International are used to advance mobility engineering throughout the world. The SAE Technical Standards Development Program is among the organization's primary provisions to those mobility industries it serves aerospace, automotive, and commercial vehicle. These works are authorized, revised, and maintained by the volunteer efforts of more than 9,000 engineers, and other qualified professionals from around the world. SAE subject matter experts act as individuals in the standards process, not as representatives of their organizations. Thus, SAE standards represent optimal technical content developed in a transparent, open, and collaborative process.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1 and the SAE Technical Standards Board Policy. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and SAE International shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

© ISO/SAE International 2021

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO or SAE International at the respective address below or ISO's member body in the country of the requester.

ISO copyright office CP 401 • Ch. de Blandornet 8 CH-1214 Vevey, Geneva Phone: +41 22 748 01 11 Fax: +41 22 748 00 47 Email: copyright@iso.org Website: www.iso.org	SAE International Tel: 877-606-7323 (inside USA and Canada) Tel: +1 724-776-6070 (outside USA) Fax: 724-776-6790 Email: CustomerService@sae.org SAE WEB ADDRESS: http://www.sae.org
---	--

Published in Switzerland and USA

ECE/TRANS/505/Rev.3/Add.154

4 March 2021

INTERNATIONAL STANDARD ISO 26262-1

Second edition
2018-12

Adoption of Harmonized Technical United Nations Regulations* for Wheeled Vehicles, Equipment and Parts which can be Used on Wheeled Vehicles and the Conditions for Recognition of Approvals Granted on the Basis of these Regulations*

ing the amendments which entered into force on 14 September 2017)

UN Regulation No. 155
force as an annex to the 1958 Agreement: 22 January 2021

Road vehicles — Functional safety — Part 1: Vocabulary

véhicules routiers — Sécurité fonctionnelle — Partie 1: Vocabulaire


UNITED NATIONS

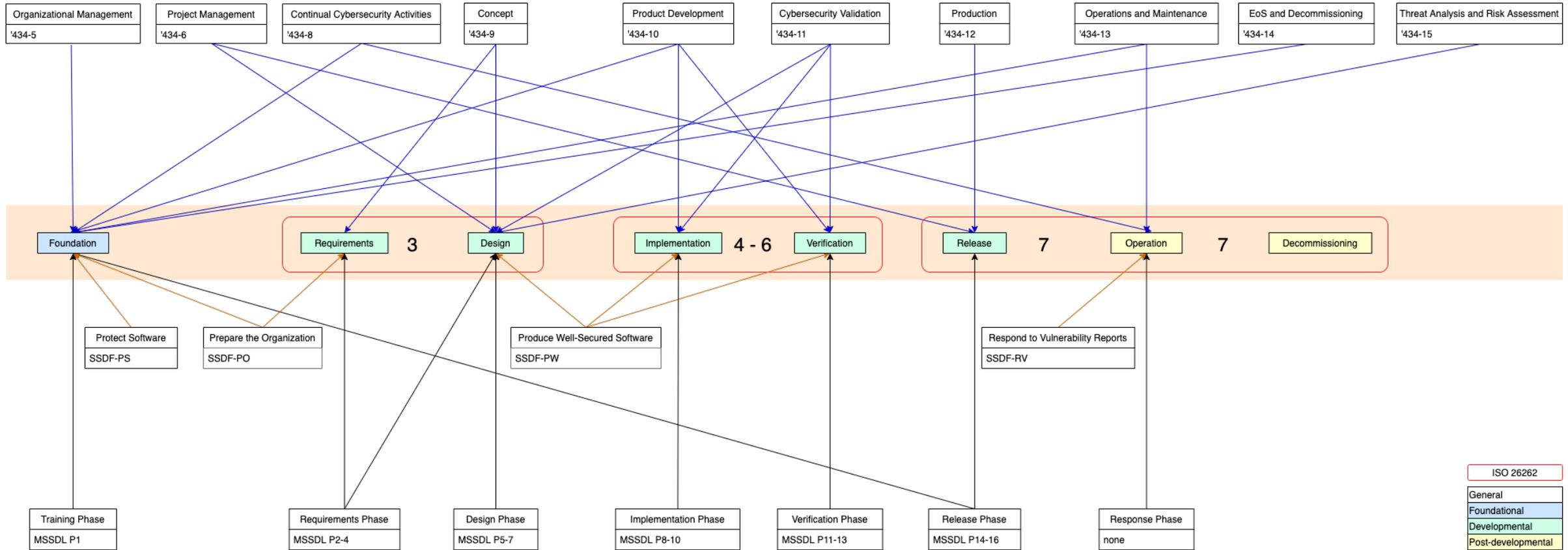
Reference number
ISO 26262-1:2018(E)

© ISO 2018

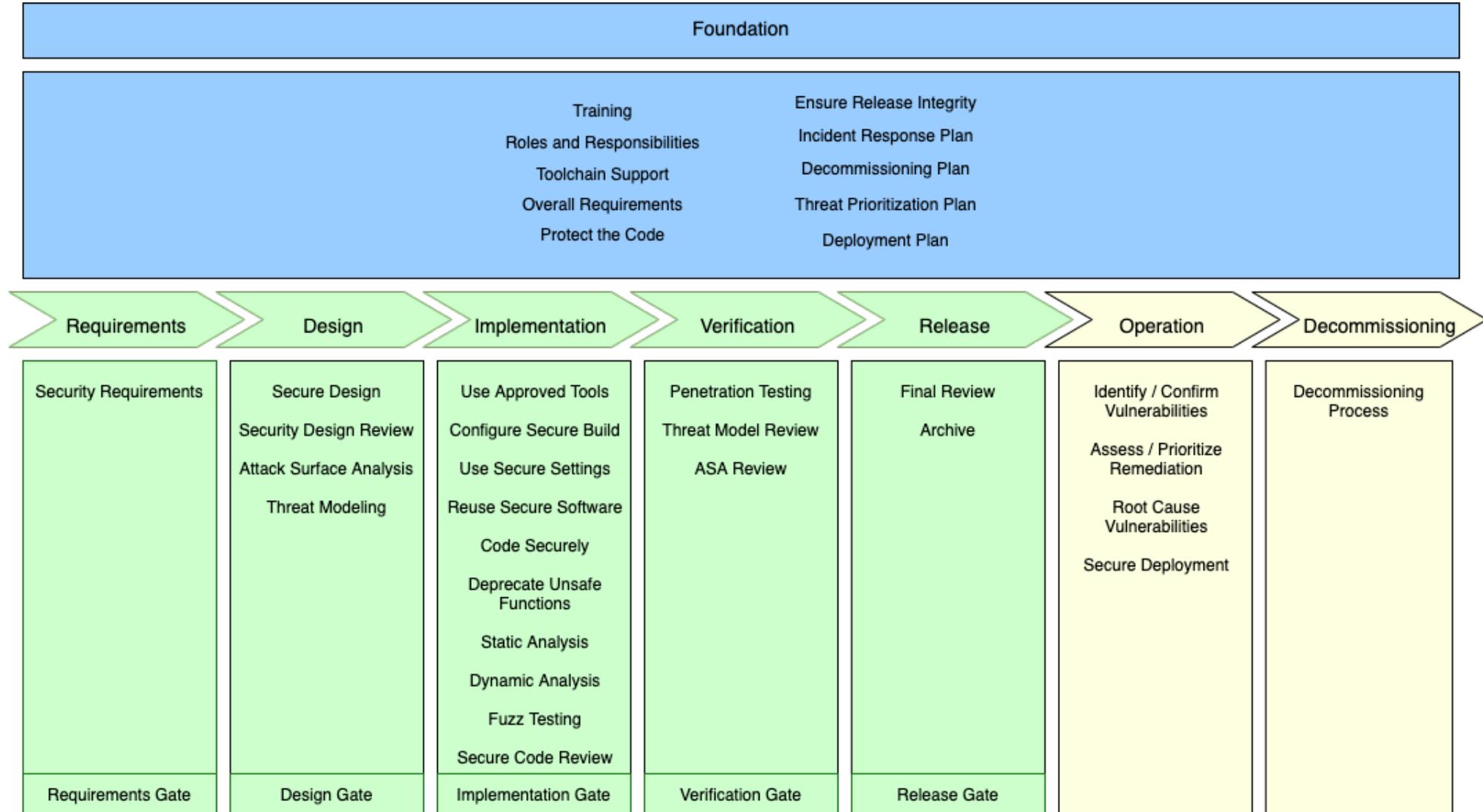
AVPDL – Autonomous Vehicle Product Development Lifecycle

AVPDL	15288 (SDLC system)	12207 (SDLC software)	26262 (safety)	21434 (cybersecurity)
organization processes	technical processes	technical processes	management of functional safety	overall cybersecurity management
			supporting processes	project dependent cybersecurity management
foundation phase	N/A	N/A	concept phase	concept
requirements phase	requirements definition	requirements definition	safety requirements	cybersecurity requirements
	requirements analysis	system requirements analysis	hazard analysis / risk assessment	cybersecurity assessment
design phase	architectural design	system architectural design	architectural design	cybersecurity design
implementation phase	implementation	implementation	implementation	development
	integration	system integration	integration and verification	integration and verification
verification phase	verification	system qualification testing		
	transition	software installation		
release phase	validation	software acceptance support	production	production
		operation		
operation phase	operation	software operation	operation, service and decommissioning	continuous cybersecurity activities
	maintenance	software maintenance		operation and maintenance
decommissioning phase	disposal	software disposal	decommissioning	decommissioning
supplier processes	agreement processes	agreement processes	supporting processes	distributed cybersecurity activities

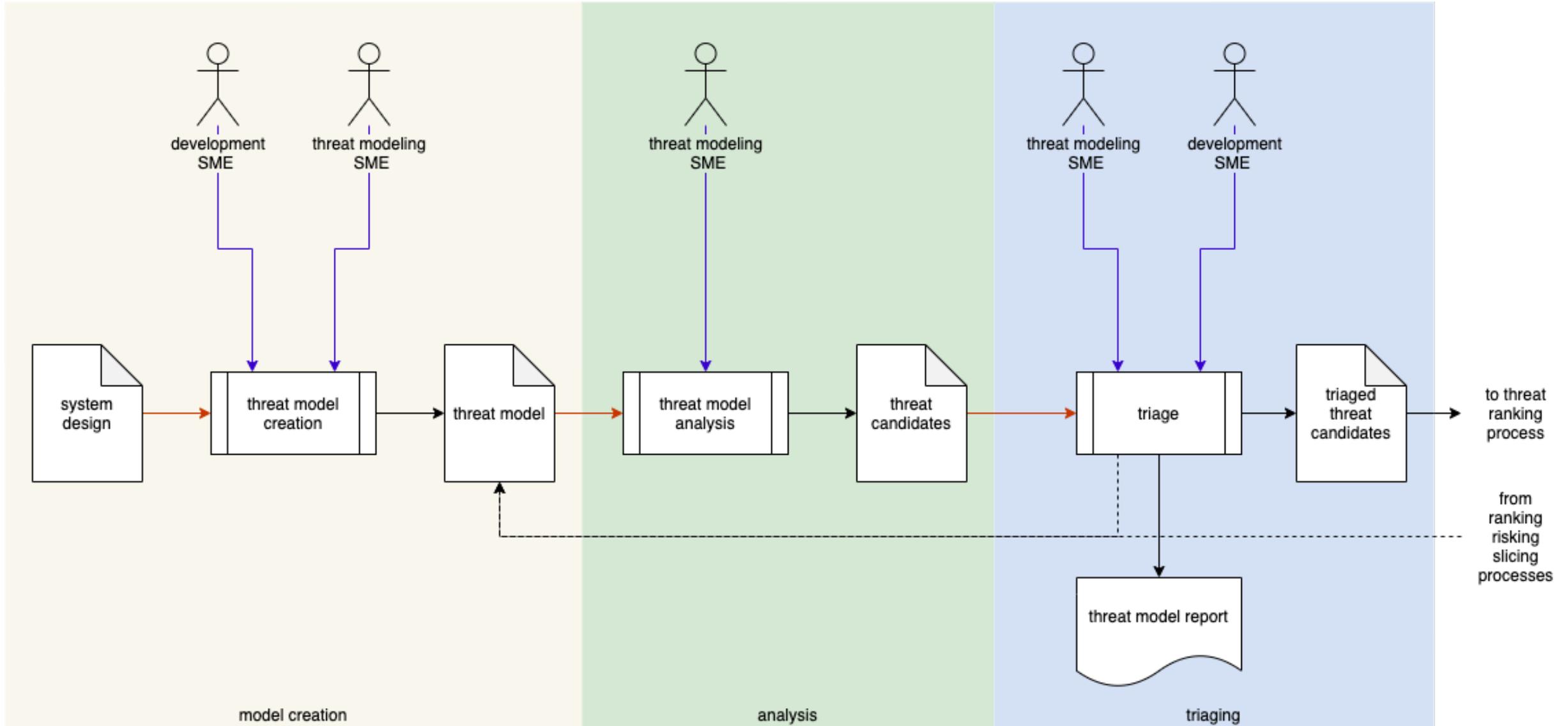
How Standards Inform the AVCDL



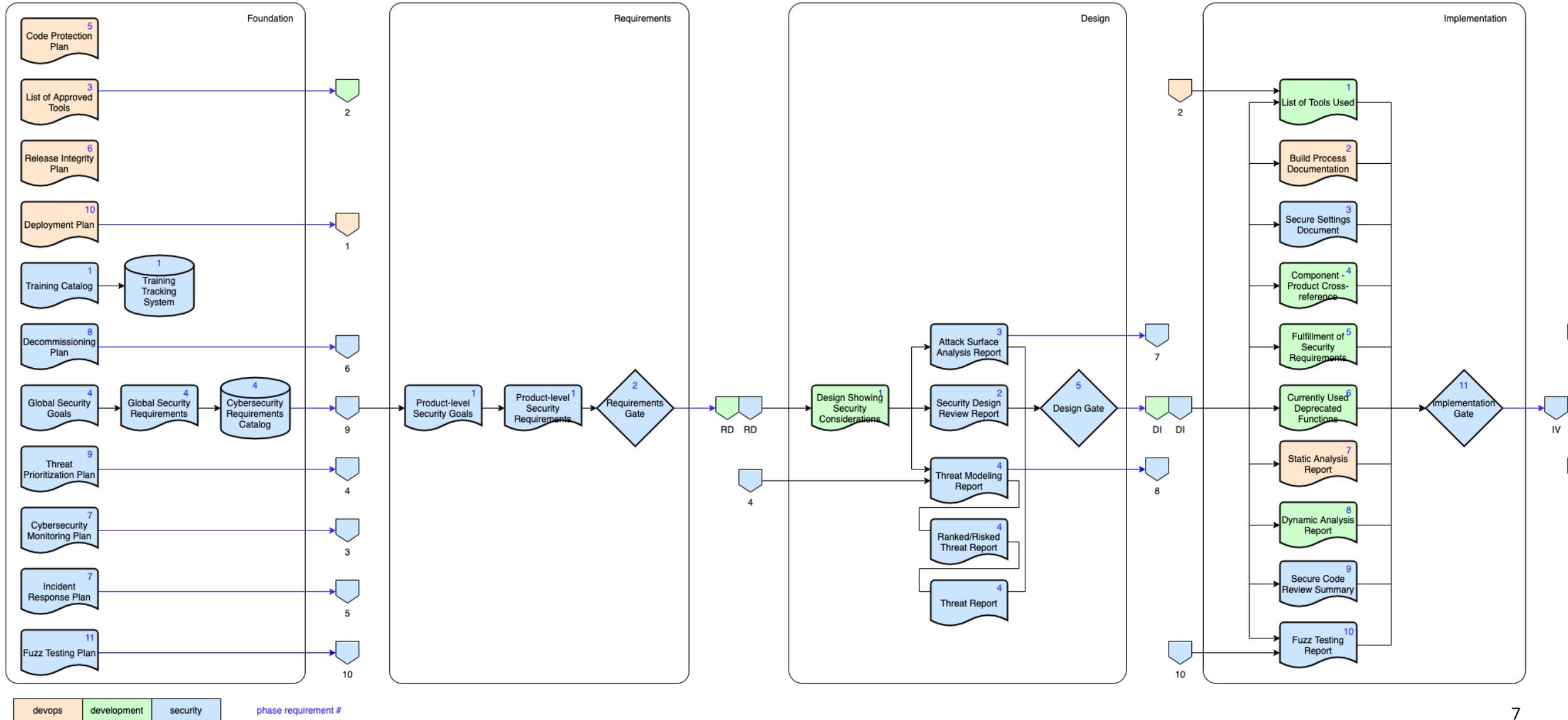
Phases and Requirements



Process Flows



Traceability



AVCDL on GitHub

nutonomy / AVCDL Public

Watch 3 Fork 1 Star 15

Code Issues Pull requests Actions Wiki Security Insights Settings

main 1 branch 59 tags

Go to file Add file Code

About

This repository contains material related to the Autonomous Vehicle Cybersecurity Development Lifecycle (AVCDL)

cybersecurity autonomous-vehicles development-lifecycle avcdl iso21434

Readme View license 15 stars 3 watching 1 fork

Releases 50

2.4.3 Latest 4 days ago

+ 49 releases

Packages

No packages published
[Publish your first package](#)

Motional-Charles-Wilson added Code Signing secondary document / updated ... b220d59 4 days ago 89 commits

background_material	added supplier cybersecurity maturity blog post	last month
distribution	added Code Signing secondary document / updated Code Protection...	4 days ago
source	added Code Signing secondary document / updated Code Protection...	4 days ago
.gitignore	created .gitignore	4 months ago
LICENSE.md	moved license up a level	8 months ago
README.md	added note for Windows users and long FQPNs	14 days ago
document status.md	added Code Signing secondary document / updated Code Protection...	4 days ago
mentions.md	added mentions page	2 months ago

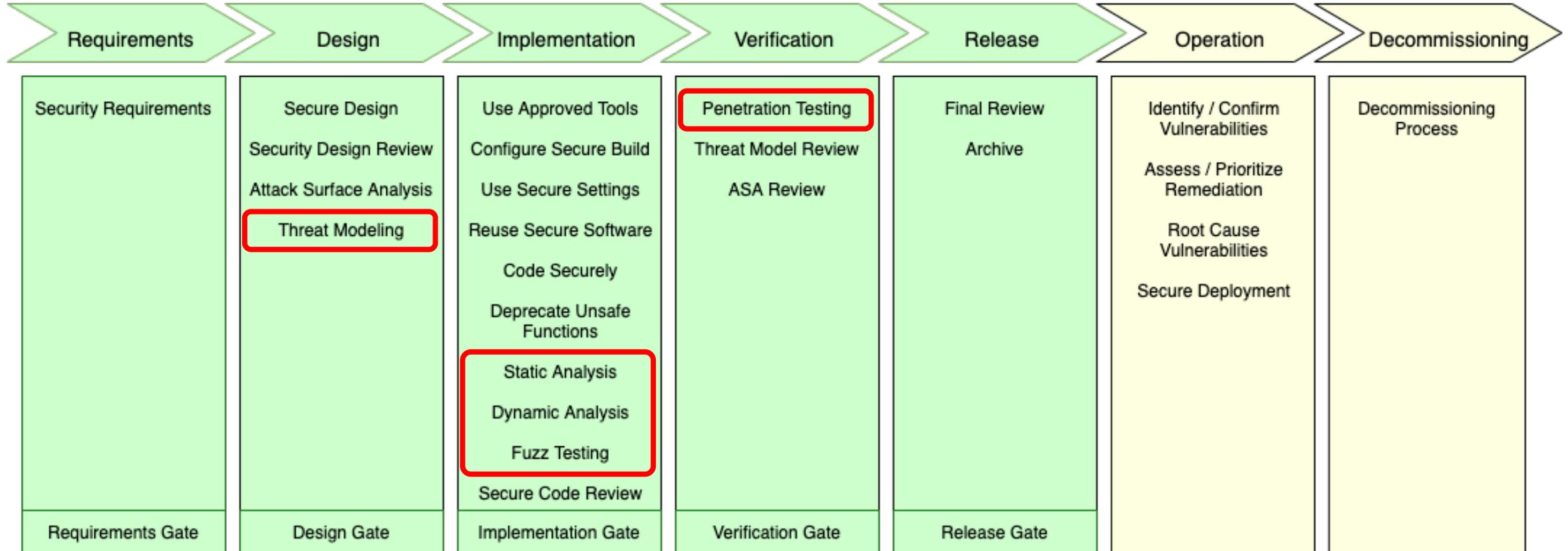
README.md

AVCDL

Overview

The AVCDL is a set of identified processes, requirements of those processes, generated products, and mappings from the generated products to their corresponding certification standard (ISO/SAE 21434, UNECE WP.29 R155-7) work products: for the purpose of ensuring the creation of secure systems.

SARIF-relevant Processes



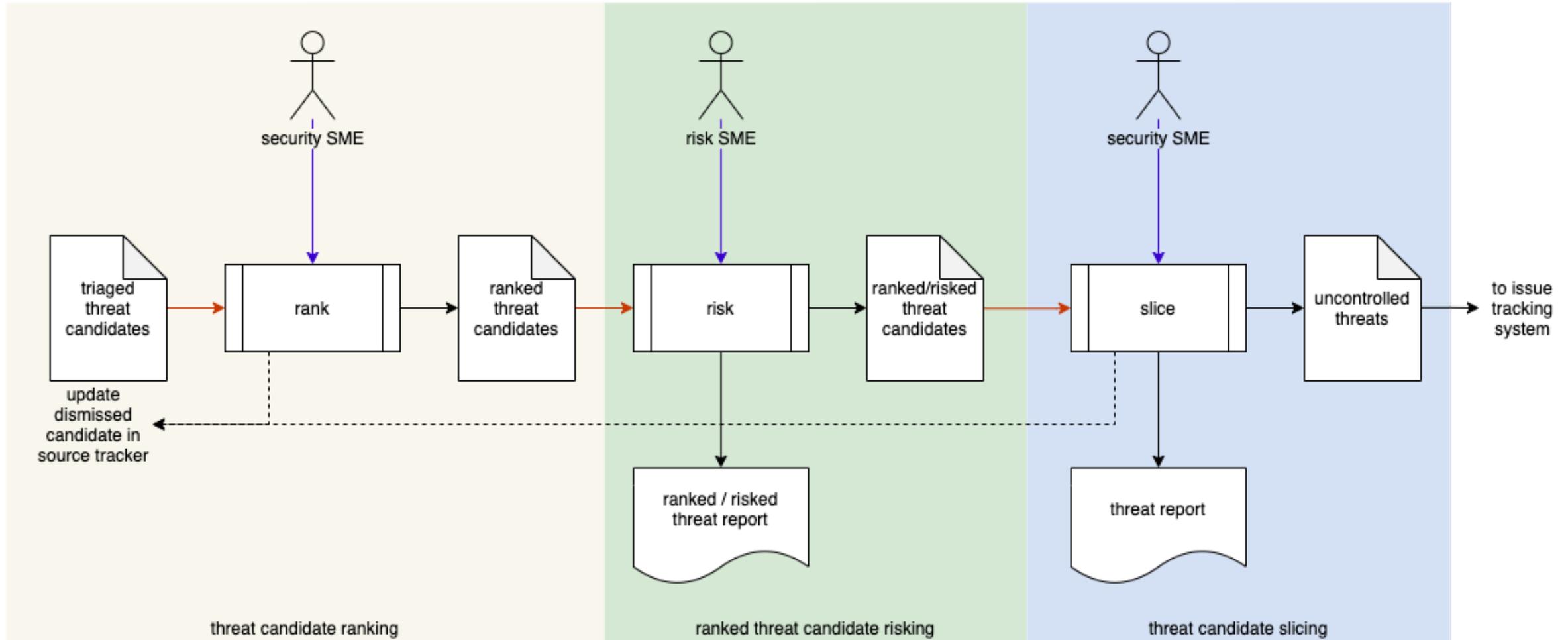
SARIF Field Compatibility

Process	SARIF element				
	Context	Run	Test	Finding	
				Location	Issue
Static Analysis	Common	Common	Checker	File / Line	Violation
Threat Modeling			Rule	Graph Edge	Violation
Fuzz Testing			Checker	File / Line	Fault
Dynamic Analysis			Checker	(variable resolution location)	Failure
Penetration Testing			Test	Test Step	Failure

Why Extend SARIF? (Static → Systematic)

- **Body of Knowledge (standard and practitioners)**
- **Automation**
- **Consistency**
- **Scale**
- **Supply Chain (data interchange)**
- **Single Source of Truth**

Consistency – Threat Prioritization Process



References (1 of 2)

Systems and software engineering - Software life cycle processes

https://en.wikipedia.org/wiki/ISO/IEC_12207

Systems and software engineering - System life cycle processes

https://en.wikipedia.org/wiki/ISO/IEC_15288

Road vehicles – Functional safety

https://en.wikipedia.org/wiki/ISO_26262

Secure Software Development for Autonomous Vehicles

<https://www.sae.org/standards/content/iso/sae21434/>

Microsoft Security Development Lifecycle (SDL) - simplified implementation

<http://download.microsoft.com/download/F/7/D/F7D6B14F-0149-4FE8-A00F-0B9858404D85/SimplifiedImplementationoftheSDL.doc>

NHTSA Cybersecurity Best Practices for the Safety of Modern Vehicles

https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf

NICE Cybersecurity Workforce Framework (NCWF)

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf>

References (2 of 2)

Secure Software Development Framework (SSDF)

<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04232020.pdf>

AVCDL (GitHub)

<https://github.com/nutonomy/AVCDL>

AVCDL Introductory Blog Post

https://github.com/nutonomy/AVCDL/tree/main/background_material/blog_posts

UN Regulation No. 155 - Cyber security and cyber security management system

<https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security>